Teka of Political Science and International Relations – OL PAN/UMCS, 2018, 13/2, 115–128
DOI: 10.17951/teka.2018.13.2.115-128

THE FUTURE OF THE INTERNET – THE TRAPS OF FORECASTING. THE INTERNET OF THINGS AND AUGMENTED REALITY IN A MILITARY CONTEXT

Dominika Dziwisz
Jagiellonian University. Institute of Political Sciences and International Relations
ORCID ID: https://orcid.org/0000-0002-5837-3446
e-mail: dominika.dziwisz@gmail.com

Abstract: Modern information technologies are double-edged weapons, because on the one hand, they provide a huge tactical advantage, but on the other, they are a source of many dangers. Therefore, when designing the most effective solutions in the field of IT security, one should examine contemporary trends and anticipate possible scenarios concerning the future of the Internet and online tools, because solutions suited to the current conditions may be ineffective in the future. This is due not only to technological factors related to the development of computer hardware or software, but also to decisions, cooperation and competition. It is impossible to specify all the factors that will determine the future of the Internet. Therefore, the author's intention is to pay attention to only a few, subjectively selected tendencies. The aim of the article is indicating the possible directions of development of two Internet technologies – the Internet of Things and Augmented Reality, and analysing possible mistakes that could be made in the process. The second research goal is to identify threats that are a consequence of the more frequent and wider use of both technologies.

Keywords: Internet of Things, Internet, Augmented Reality, state security

INTRODUCTION

Nikola Tesla, today regarded as one of the greatest inventors of all time, who was once a misunderstood genius, said the following words in an interview with *Collier's* magazine in 1926:

> […] When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole. We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles [Kennedy 1926].

Decades later, Tesla's prophecy became a reality.

Many inventions, including Tesla's, were created for military purposes, and only later found their civil use. The best known example is the satellite navigation system (Global Positioning System, GPS) created in the early 1990s by the Department of Defense of the United States. The system has many civil uses today, for example, it is used in applications such as Google Traffic, i.e. an online traffic tracking service, or iTaxi for ordering transport services. Other examples of technologies whose primary purpose was a military one are freeze drying, computers, microwaves, walkie-talkie, night vision, nuclear technology, and even duct tape. The Internet was also first created for military purposes.

In the early 1960s, Paul Baran, a RAND Corporation scientist managed to design a command and control system – a resistant communications network based on packet switching, i.e. data transmission conducted by dividing data into smaller parts [Laperche, Uzunidis, von Tunzelmann 2008]. Thanks to this property, even if one communication node was destroyed, another node could take over its function [Dziwisz 2015: 65–67]. This created the foundations of computer networks, including today's Internet. In 1969, this technology was used by an internal unit of the U.S. Department of Defense – Advanced Research Projects Agency (ARPA) to create Arpanet, the precursor of today's Internet. In the same year, the first data bit was transmitted.

Today the Internet is almost fifty years old. Its history is both interesting and instructive, but predicting the future of the Internet is definitely a more fascinating challenge, albeit a much more difficult one, especially that currently the catalyst for new inventions are no longer the needs of the army. In many cases, it is not the military, but the private sector that is the driving force of inventions used for military purposes. Quite often gadgets from the commercial market are more technologically advanced than military ones [Zheng, Carter 2015]. Increasingly, the state sector is using commercial technology, and not vice versa. This does not mean, of course, that the military and the state sector have ceased to be innovative. Indeed, the army equips both its civilian and military employees with devices offering the functionalities of commercially available smartphones, but is still a leader in the development of certain advanced applications of Internet of Things technologies, such as monitoring and reconnaissance drones or advanced sensors and satellite communication systems [Zheng, Carter 2015].

Modern military operations are carried out in a dynamic and multidimensional environment, and military commanders operate under strong time pressure. Therefore, an accurate assessment of the situation, possible directions of action and decision-making must be immediate. Hence, for a complete and reliable picture of the situation in near-real time, one needs to draw from all possible sources of information. One of the answers to these challenges are modern Internet technologies, such as the Internet of Things (IoT) and Augmented Reality (AR). However, the integration of heterogeneous sensors and systems that differ in

technology, as well as an effective combination of the capabilities of both these technologies is a problem not only for military entities.

When designing the most effective solutions in the field of IT security, one should examine contemporary trends and anticipate possible scenarios concerning the future of the Internet and online tools, because solutions suited to the current conditions may be ineffective in the future. This is due not only to technological factors related to the development of computer hardware or software, but also to decisions, cooperation and competition. It is impossible to specify all the factors that will determine the future of the Internet. Therefore, the author's intention is to pay attention to only a few, subjectively selected tendencies. The aim of the article is indicating the possible directions of development of two Internet technologies – the Internet of Things and Augmented Reality, and analysing possible mistakes which could be made in the process. The second research goal is to identify threats that are a consequence of the more frequent and wider use of both technologies.

DEFINITION AND APPLICATION OF THE IOT AND AR IN THE ARMY

Walt Mossberg, a journalist and expert in the field of modern information technologies, defined the Internet of Things as

> […] a whole constellation of inanimate objects […] with built-in wireless connectivity, so that they can be monitored, controlled and linked over the Internet via a mobile app. And many of these sensors and connected objects can be installed in the home without changing wiring or hiring a professional [Mossberg 2014].

This popular definition reflects how the IoT is widely understood. Most people associate the IoT with various devices that monitor our physical activity, autonomous cars, or even modern refrigerators that can order shopping from the store, but, in fact, the IoT is much more – for example, intelligent meters that enable better management of energy and water resources, sensors monitoring and automating production halls, intelligent systems controlling the operation of jet engines, modern solutions for the army, and even devices allowing better diagnosis of diseases. In addition, we are rarely aware that the IoT can connect not only inanimate objects but also plants, animals and even people. For example, a company called Sparked has developed a method for tracking cows using radio positioning sensors that are implanted in their ears. This allows farmers to monitor animal health and track their movements. It is estimated that each cow generates about two hundred megabytes of information per year [*It's a Smart World*... 2010]. Because of such ambiguities, the IoT is called by some "the Internet of Everything" (IoE), because it refers not only to things, but also people, places and objects [LOPEZ Research 2013].

It is difficult to accept one date as the beginning of the IoT – it might be the moment when more things or objects were connected to the Internet than the population of the world. If in 2003 Earth had ca. 6.3 billion people, and the Internet connection was around 500 million devices, there was ca. 0.08 device per person. It should therefore be recognized that the IoT did not exist at the time. Its beginnings date back to around the year 2008 [CISCO 2011]. As estimated, in 2020, approx. 50 billion devices will be connected to the Internet [CISCO 2011]. It is worth noting that this calculation does not take into account the rapid progress in Internet technology or the development of the devices themselves. The figures presented are based on what we know now.

One can also assume that the origins of the IoT date back to the early 1990s. At that time, the U.S. Department of Defense developed the concept of "network-centric warfare" (NCW) [Alberts, Garstka, Stein 1999]. These were war activities aiming at achieving information advantage for increasing the army's combat capabilities. In order to achieve such an advantage in the era of modern information technologies, it is necessary to use advanced systems for the exchange of information and the integration of data collected from geographically dispersed sensors [Sienkiewicz, Świeboda 2009]. In other words, network-centric war consists in the integration of activities in three domains: physical, i.e. the actual place of operations where information is collected both by sensors and in a traditional way; information, where data is transmitted and stored, and cognitive, where data processing and analysis takes place [Zheng, Carter 2015]. Solutions developed for the concept of network-centric war directly translate into the foundations of today's IoT.

The American Defense Information Systems Agency (DISA) in its strategic plan for the years 2014–2019 entered the IoT on list of *technologies to watch* [*Strategic Plan 2014–2019*... 2014]. It was emphasized that the IoT will have an impact on everything that the Department of Defense and the army deals with, from qualitatively better supervision of logistics through optimized building safety and environmental inspections to monitoring the health of individual soldiers. However, despite the prioritization of IoT technologies, its military use so far has been limited and boils down to implementing C4ISR command support systems (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). The IoT has also been used in some applications for logistics management as well as trainings and simulations [Zheng, Carter 2015]. An example of using the IoT in the army would be helmets with built-in sensors to help diagnose brain damage or DARPA-developed robotic limbs for soldiers wounded on the battlefield, or portable computer technologies that can be built into combat uniforms [Seffers 2015; Singer 2010].

The other technology to be analysed is Augmented Reality (AR). In 1994, the scientists Paul Milgram and Fumio Kishino described the area located between what is real and what is virtual [Milgram, Kishino 1994]. The concept of mixed reality (MR) which they developed has evolved to AR, in other words, a reality in which the digital layer is imposed on the real and physical one. Thus, AR is a sys-

tem that combines real-time world with computer-generated one. AR interfaces impose textural or pictorial information on images captured in 3D technology and thus enable users to interact with the real and virtual element at the same time. In contrast to virtual reality, which creates a completely artificial environment, AR uses the existing environment and imposes new information on it. Hence, the technical challenge in AR technology is to determine in real time what elements of the image should be shown, where and how [Koniarski 2015]. Two current examples of popular AR applications are Snapchat, a mobile application for sending videos and photos to which AR filters may be added, and *Pokémon Go*, a city game in which the player, thanks to AR, has the ability to "catch" a Pokémon appearing on the screen of his/her smartphone. Another application of AR are virtual lines in the broadcasts of football matches.

AR is increasingly used in the army. For example, modern soldiers use a system similar to Google Glass, but intended for use on the battlefield. The ARC4 software, developed at the request of the DARPA agency, allows commanders to send maps and other information directly to the soldier's field of vision. The system may also display key information such as the location of enemies, satellite materials and mission objectives. The user of glasses can also indicate targets and inform the command of operations concerning these, and even provide an image from his built-in camera. The command can at any moment also look at the battlefield from the perspective of the chosen soldier [Mrożewski 2016]. ARC4 not only allows the soldier to acquire time-critical tactical information, but above all, the soldier does not have to check maps or other devices to access it. Thanks to this, the attention of soldiers is not diverted from what is happening directly in front of them.

More advanced use of AR in the army was presented in 2017 at the international weapons fair in London in the form of CV90 infantry combat vehicle [Lynch 2017], which thanks to AR technologies is to ensure more efficient combination of data transmitted from sensors and accelerate their processing in real time. In practice, CV90 "armed" with modern sensors and imaging systems will allow soldiers inside the car to see the external situation as if they were moving in a transparent box. Consequently, the soldier, instead of leaning outside the vehicle to do reconnaissance and serve a machine gun, will have AR goggles that will allow him to get a 360-degree view of the battlefield. In addition, thanks to AI image recognition systems with access to large "threat libraries", which send information whether the object is an enemy or not, soldiers will be able to track other participants on the battlefield [Lynch 2017].

The above and other examples show that army solutions are powered by the same technology as commercial mobile applications such as Snapchat. In other words, the technology used for entertainment has also found application in the process of taking life-or-death decisions. This demonstrates the versatility of AR both as a tool for maintaining peace and security (e.g. software for aviation or emergency services), as well as for waging war (modern types of weapons).

IOT AND AR IN THE ARMY – THREATS AND FORECASTING PROBLEMS

Niels Bohr said that "prediction is very difficult, especially about the future" [Ellis 1970]. Truly, usually when one tries to predict the future, one as if freezes time – takes a trend and considers its functioning in a society exactly the same as it is today. It is a trap that is difficult to avoid. Additionally, analysing individual technological trends in isolation from other trends is doomed to a failure. It is no different in the case of the IoT and AR, the possibilities of which have been analysed separately many times.

As shown above, both the IoT and AR have found more and more applications in the military. There are many possible examples of combining the possibilities of both technologies if AR acts as an interface for IoT objects. To understand this, it is enough to realize that the world around us is represented in our brains as an image. What AR does exactly is that it takes an existing image and blends it with some new information. In other words, by combining the capabilities of AR and the IoT, the environment becomes more responsive and also possible to manage remotely. Detailed 3D maps of the physical environment in real time available at the soldier's fingertips are a good case in point here. Another one may be a rifle which automatically gives the soldier information about the state of ammunition and cylinder temperature, so that they can send information that fire support is needed.

The September 2015 report of the American Center for Strategic and International Studies (CSIS) highlights the greatest risks related to the use of the IoT in the army [Zheng, Carter 2015]. The IoT, by default in conjunction with AR, can be used to collect and transmit sensitive data, e.g. regarding position, deployment of troops and equipment, support units, or inventory resources, enabling the opponent to anticipate the movements of U.S. forces. Therefore, the first danger resulting from the use of Internet technologies is the risk of the enemy acquiring sensitive data that will give them a tactical advantage. In other words, the use of the IoT makes systems more vulnerable to electronic warfare. One of the possible consequences may be disclosing the position of military units through transmitters located in IoT devices. As revealed in early 2018, the U.S. and British military equipped thousands of their soldiers with electronic fitness bands connecting to the Strava application as part of a pilot program to fight obesity [Sly 2018]. Strava uses GPS data to determine the location and movement of 27 million users of services, including fitness applications, as well as GPS wristbands and other wearables, such as Fitbit and Jawbone. The map of activity of users of fitness wristbands generated and posted on the Internet revealed sensitive information about the location and activities of soldiers in military bases in Africa, Afghanistan, and Syria.

Secondly, sensitive information may not only be obtained by the enemy, but the enemy can manipulate or interfere with the transmission of information between individuals. The effects of such actions could be diverse: giving the

commanders an incorrect picture of the actual situation, suspending the work of the electronic parts of the weapon or the failure of network management systems.

Thirdly, vulnerabilities in security could allow the enemy to take control of or block automated systems, which would prevent individuals from carrying out their missions, and could even make them use their resources against each other. This means that if military networks are not sufficiently secured, "U.S. guns, missiles, and bombs may not fire, or may be directed against our own troops. Resupply, including food, water, ammunition, and fuel may not arrive when or where needed" [Resilient Military Systems… 2013].

Finally, ensuring IT security is a challenge for all organizations and that is why training all employees, not only technical ones, is an important task. There is a risk of excessive confidence in IoT and AR technologies and related underestimation of personnel costs. As long as the military does not understand that new technologies require new skills and highly qualified staff, it will not be possible to use them consciously and safely. The U.S. Department of Defense employs 3 million people including civilians, active and reserve soldiers and national guard. Even the smallest human mistake can prove dangerous, because knowing complicated hacking techniques is not necessary to gain access to the network. As more and more security technologies are invented that make it difficult to find technical gaps in the system, attackers will attempt to target human weakness. Breaking the "human barrier" is much simpler and sometimes requires only a telephone conversation [Mitnick, Simon 2003]. For this reason, it is crucial to constantly improve the education level not only of IT specialists, but also of every person using the computer and the Internet.

The threats indicated in the CSIS report do not exhaust the list of potential dangers related to the use of the IoT and AR. It is also worth paying attention to the changes that are associated with the use of the IoT and AR in the army in a wider context. First of all, one must keep in mind that the number of IoT devices will increase, which means that the number of access points to the systems will also be higher. Due to the need for communication, IoT devices will be connected to a common network. Most of them will be well secured, but with the growing number of devices there will also be those that will be updated less often; in fact, now some IoT devices are actually unable to update some of their subsystems. Considering the fact that vulnerabilities in low-level components or even communication protocols are still being discovered, it is impossible to secure all devices. This, in turn, raises the risk that less critical and less secure IoT devices will become a gateway into the system for hackers and a starting point for attacking other, more important targets. A good example of this phenomenon is BlueBorne, a vulnerability in the Bluetooth protocol itself, as it will affect all non-updated Bluetooth devices. If any of them (e.g. a portable speaker that does not have the ability to update the embedded software) is infected, it can be used as a starting point for a more complex attack on sensitive devices in its vicinity (such as laptops or drones).

In addition, until now AR has mainly used as an interface for relatively small things, such as Google Glasses, HoloLens or some smaller drones. The latest trend is connecting larger items to the Internet (the author calls this trend the "Internet of Large Things", IoLT). An example may be the new unmanned and autonomous F-16 multirole fighter that can "think" and "fight" independently [Lockie 2017]. The new F-16 is not only able to choose the best way to shoot down a target, but also to independently carry out the shooting and landing mission. This is a complicated and extremely expensive weapon, which may lead to the simple conclusion that a hacker in this case would be able to do much more damage than in the case of a smaller reconnaissance drone, such as AeroVironment RQ-11 Raven. It also means that modern information technologies are double-edged weapons, because, on the one hand, they provide a huge tactical advantage, but on the other, they are also a source of many dangers. Therefore, the fundamental change and threat to the security of military systems is that attacking the technologies of the Internet of Big Things creates the risk of greater losses and damage. The phenomenon has been explained very well by Gen. Ronnie Hawkins Jr., director of DISA:

> […] Everybody's got a thermostat in their house – when it's tied into the Internet, how do you make sure your thermostat is secure and somebody can't just go in there and turn your thermostat down in the middle of the winter? Individuals are going to have to be much more conscious of what the Internet of Things means to them [Seffers 2015].

If you can hack a thermostat, an attack on the IoLT element is also likely. Of course, strategically important military and government networks are not connected to the Internet, but to a potentially well-secured internal network. However, in computer networks, there is no such thing as total security, so a successful attack on a military network cannot be fully ruled out.

This is confirmed by the attack of the most famous computer worm, Stuxnet, detected in 2010, whose aim was to stop the Iranian nuclear program. Both computer worms and viruses are code that has a detrimental effect on the software installed on a computer. The difference between them is that a virus, unlike a worm, is not independent. To spread, it needs a host file. A worm is a kind of virus that moves between computers automatically *via* the Internet, most often using email. However, if the public Internet is infected with a computer worm, when it is downloaded to a storage medium, e.g. a pendrive, it can be moved to the place selected by the hacker. Such a scenario was probably used to infect the Iranian network of centrifuges for enriching uranium. It is possible that an unaware employee uploaded the virus to his work computer, and then Stuxnet automatically infected the entire network. Hence the conclusion that any, even a well-secured network, can be successfully infected with malware. The only method to minimize the risk of a successful attack is to constantly improve security procedures and the software itself. The costs of such activities can be extremely high.

An important point in the debate on the security of the IoT and AR in the military concerns the establishment of security standards for cooperation with the private sector, as well as how commercial technologies may threaten the security of the state, as shown by the example of a fitness band that transmitted sensitive data on the location of military bases. In 2017, the U.S. Department of Homeland Security (DHS) also issued warnings to military authorities and government agencies against the use of drones produced by the Chinese company Da Jiang Innovations (DJI). It was detected that these drones were gathering and communicating sensitive information about U.S. critical infrastructure, as well as data on law enforcement to the Chinese [*(U) Da Jiang Innovations (DJI) Likely…* 2017]. Such information could be used by the Chinese authorities to coordinate physical and cyber attacks on the key elements of American infrastructure. In addition, according to DHS, they were used to help Chinese companies that wanted to invest in American assets such as vineyards.

Not only IoT devices with commercial applications can be dangerous – those that are purchased by the military from private companies may be as well. Civil electronics market is ruled by different laws than those that apply to the market of military electronics. The goal of the private sector is to reduce costs and generate profits, which is not always accompanied by meeting strict security standards [Piątek 2006]. Commercial Internet of Things technologies are developing quickly and constantly, but the processes of procuring them by the army are, however, long and complex. This is because in most cases products and services available commercially (as commercial off-the-shelf, COTS) do not provide a level of security that meets military requirements. It is so because many commercial IoT solutions offered have been designed primarily for convenient use, without rigorous security checks. The main problem therefore is finding solutions that will allow to take advantage of innovations from the commercial market while maintaining appropriate security standards. On the other hand, the bar associated with the quality and reliability required by the military may be set too high for COTS producers, and consequently hamper their cooperation [Piątek 2006]. Finding a golden mean in this situation is not easy, but if the military wants to develop new IoT and AR solutions, cooperation with the private sector is inevitable [*Maintaining NATO'S Technology…* 2017].

CONCLUSIONS

The number of potential applications of modern information technologies, such as the IoT and AR, is infinite. According to the vision of future military operations, these technologies will enable the military to carry out missions in an even more effective way, and mobile devices and communications will allow scattered operators and staffs to cooperate as if they were in the same place [*Capstone Concept for…* 2012]. Implementation of this plan will require significant investments in technology as well as specialized personnel and even changes in management culture. However, as mentioned above, Internet tools are double-edged weapons, because, on the one hand, they can give an advantage over the opponent, but on the other hand, they become a source of new dangers. Therefore, for the reasons mentioned in the article, military authorities must understand the implications of using the IoT and AR for security issues and honestly answer the three basic questions concerning risk analysis:

1. What can go wrong with the use of IT technology data? Since more and more types of devices, not excluding the Internet of Big Things, will be connected to the Internet, our vulnerability to cyber attacks will also grow.

2. What is the probability of cyber attacks? One can control the probability of attacks to a certain extent, increasing defence capabilities.

3. If there is a cyber attack, what are its potential consequences? It cannot be denied that the consequences of cyber attacks will be increasingly severe, as more critical systems become interdependent.

As shown in the Vodafone report [Vodafone 2016], 28% of companies that responded to the survey have already implemented technologies of the IoT. As many as 76% respondents recognize that the IoT will be critical to the future success of any organization in their sector. Erik Brenneis, director of Vodafone for the IoT is of the opinion that the question is not any more if a company should use the IoT, but how it should use it [Vodafone 2016]. This means that the widespread use of the IoT in the commercial world is becoming a fact. Also the armed forces of individual countries are starting to use IoT and AR technologies. However, in order to win future wars it is necessary not only to fully understand the potential benefits of these IT technologies, but also to become aware of the increasing vulnerability to cyber attacks. Unfortunately, such a risk is not static, because it is impossible to stop technological progress. Therefore, the military will have to keep fighting to keep it at an acceptable level.

Tytuł: Przyszłość Internetu – pułapki prognozowania. Internet Rzeczy i Rzeczywistość Rozszerzona w kontekście militarnym

Streszczenie: Nowoczesne technologie informatyczne są bronią obusieczną, bo z jednej strony dają ogromną przewagę taktyczną, ale z drugiej są źródłem wielu niebezpieczeństw. Dlatego projektując najbardziej skuteczne rozwiązania w zakresie bezpieczeństwa informatycznego, należy badać współczesne trendy oraz przewidywać możliwe scenariusze przyszłości Internetu i narzędzi internetowych, bo rozwiązania przystosowane do obecnych warunków mogą być nieskuteczne w przyszłości. Mają na to wpływ m.in. czynniki technologiczne związane z rozwojem sprzętu komputerowego czy oprogramowania, a także decyzje, współdziałanie oraz współzawodnictwo. Wyznaczonym w artykule celem badawczym jest wskazanie możliwych kierunków rozwoju dwóch technologii internetowych – Internetu Rzeczy i Rzeczywistości Rozszerzonej – oraz błędów popełnianych przy prognozowaniu ich przyszłości. Drugim celem badawczym jest rozpoznanie zagrożeń będących konsekwencją coraz częstszego i szerszego stosowania obu technologii.

Słowa kluczowe: Rzeczywistość Rozszerzona, Internet Rzeczy, Internet, bezpieczeństwo państwa

REFERENCES

1. Alberts D.S., Garstka J.J., Stein F.P. (1999), *Network Centric Warfare: Developing and Leveraging Information Superiority*, National Defense University Press, Washington D.C.
2. *Capstone Concept for Joint Operations: Joint Force 2020*, U.S. Joint Chiefs of Staff, September 10, 2012, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/ccjo_jointforce2020.pdf?ver=2017-12-28-162037-167 [access: 14.03.2018].
3. CISCO, *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, April 2011.
4. Dziwisz D. (2015), *Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne*, Sowa Druk, Kraków.
5. Ellis A.K. (1970), *Teaching and Learning Elementary Social Studies*, Allyn and Bacon, Boston, p. 431.
6. *It's a Smart World. A Special Report on Smart Systems*, "The Economist", November 6, 2010, http://www.economist.com/sites/default/files/special-reports-pdfs/17408526.pdf [access: 23.03.2018].
7. Kennedy J.B. (1926), *When Woman is Boss. An Interview with Nikola Tesla by John B. Kennedy*, "Collier's", January 30 (own translation).
8. Koniarski K. (2015), *Augmented reality using optical flow*, "Annals of Computer Science and Information Systems", vol. 5, pp. 841–847. DOI: https://doi.org/10.15439/2015F202.
9. Laperche B., Uzunidis D., von Tunzelmann G.N. (2008), *The Genesis of Innovation. Systemic Linkages Between Knowledge and the Market*, Edward Elgar Publishing, Cheltenham, pp. 120–125.
10. Lockie A. (2017), *The Air Force just demonstrated an autonomous F-16 that can fly and take out a target all by itself*, April 4, http://www.businessinsider.com/f-16-drone-have-raider-ii-loyal-wingman-f-35-lockheed-martin-2017-4?IR=T [access: 20.02.2018].
11. LOPEZ Research, *An Introduction to the Internet of Things (IoT)*, November 2013, https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf [access: 1.03.2018].

12. Lynch G. (2017), *AR warfare: How the military is using augmented reality*, September 16, https://www.techradar.com/news/death-becomes-ar-how-the-military-is-using-augmented-reality [access: 20.03.2018].
13. *Maintaining NATO'S Technology Edge: Strategic Adaptation and Defence Research & Development*, 2017, NATO Parliamentary Assembly, STC General Report, https://www.nato-pa.int/document/2017-maintaining-natos-technological-edge-marino-report-174-stc-17-e-bis [access: 25.03.2018].
14. Milgram P., Kishino F. (1994), *A taxonomy of mixed reality visual displays*, "IEICE Transactions on Information Systems", vol. E77-D(12), pp. 1321–1329.
15. Mitnick K., Simon W. (2003), *Sztuka podstępu. Łamałem ludzi, nie hasła*, Helion, Gliwice.
16. Mossberg W. (2014), *SmartThings Automates Your House Via Sensors, App*, January 28, https://www.recode.net/2014/1/28/11622774/smartthings-automates-your-house-via-sensors-app [access: 21.02.2018].
17. Mrożewski B. (2016), *AR na polu walki*, „PC Format", p. 2, https://www.pcformat.pl/AR-na-polu-walki,a,4500 [access: 23.03.2018].
18. Piątek Z. (2006), *Wojskowe ze sklepowej półki*, „Elektronika B2B", July 17, https://elektronikab2b.pl/biznes/637-wojskowe-ze-sklepowej-polki-cz-1#.WrTD97aBj2R [access: 4.03.2018].
19. *Resilient Military Systems and the Advanced Cyber Threat*, Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, D.C. January 2013, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf; after: Zheng D.E., Carter W.A., 2015, *Leveraging the Internet of Things for a More Efficient and Effective Military*, CSIS, September 17, p. 20.
20. Seffers G.I. (2015), *Defense Department Awakens to Internet of Things*, "AFCEA", January 1, https://www.afcea.org/content/defense-department-awakens-internet-things (access: 20.02.2018).
21. Sienkiewicz P., Świeboda H. (2009), *Sieci teleinformatyczna jako instrument państwa – zjawisko walki informacyjnej*, [in:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, PISM, Warszawa, pp. 75–93.
22. Singer E. (2010), *Robotic limbs that plug into the brain*, "MIT Technology Review", October 27, https://www.technologyreview.com/s/421347/robotic-limbs-that-plug-into-the-brain/ [access: 23.03.2018].
23. Sly L. (2018), *U.S. soldiers are revealing sensitive and dangerous information by jogging*, "The Washington Post", January 29, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?utm_term=.eb9246385083 [access: 20.03.2018].
24. *Strategic Plan 2014–2019. VERSION 2*, Defense Information Systems Agency (DISA), https://www.hsdl.org/?view&did=753878 [access: 29.03.2018].
25. *(U) Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government*, 2017, "Intelligence Bulletin", August 9.
26. Vodafone, *The IoT Barometer* 2016, https://www.vodafone.com/business/news-and-insights/white-paper/the-iot-barometer-2016 [access: 20.03.2018].
27. Zheng D.E., Carter W.A. (2015), *Leveraging the Internet of Things for a More Efficient and Effective Military*, CSIS, September 17.